

# North Carolina Cybersecurity Awareness Month (NCSAM) Symposium

## O365 Security

**Ken Nuebler**

O365 Service Owner





# Agenda

- Is O365 Secure?
- How do we make O365 Secure for us?
- Best Practices

Is O365  
Secure?

Yes, but...





Cybersecurity is Our **Shared** Responsibility!





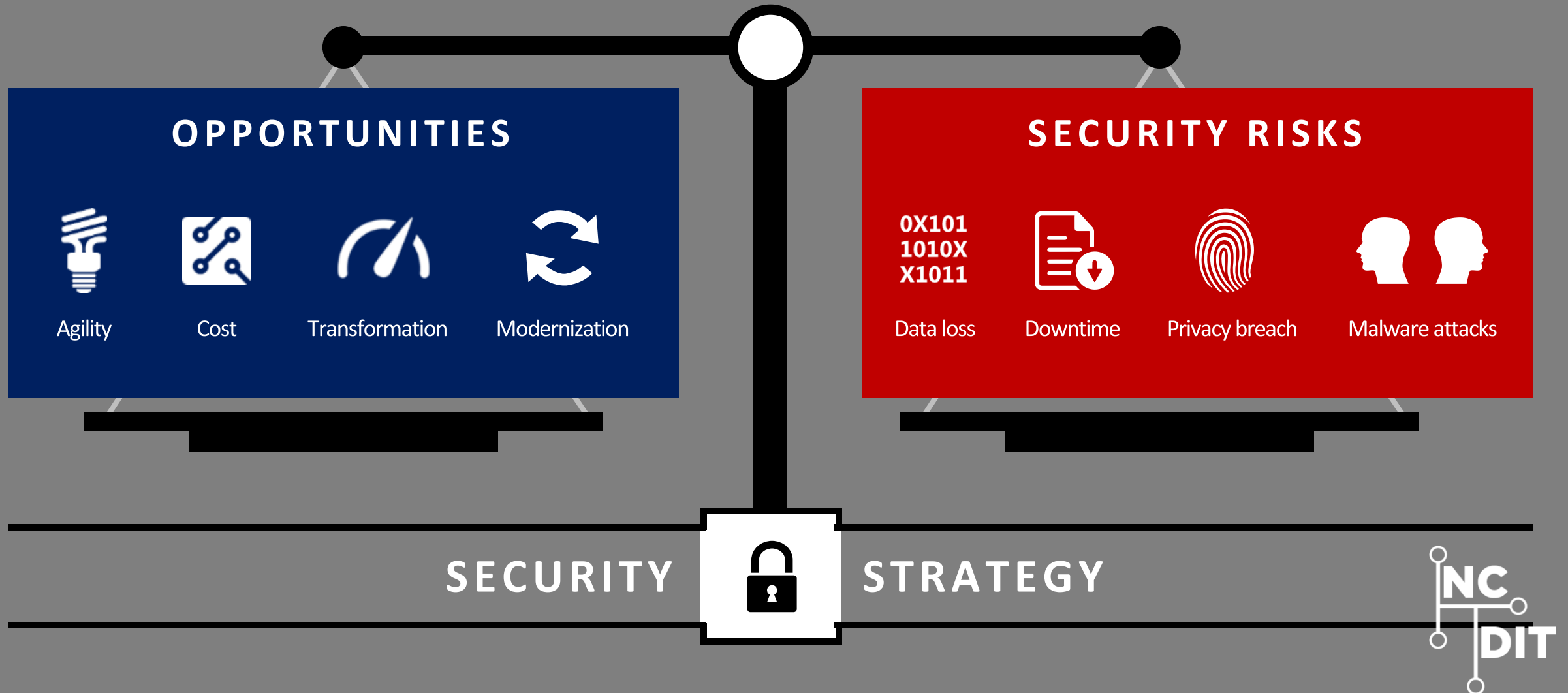
The secret to doing anything is believing that you can do it. Anything that you believe you can do strong enough, you can do. Anything. As long as you believe.

# What is Cyber Security ?

Cyber Security is a set of **principles and practices** designed to safeguard your computing assets and online information against threats

Cybersecurity is the body of **technologies, processes and practices** designed to protect networks, computers, programs and data from attack, damage or unauthorized access. In a computing context, security includes both cybersecurity and physical security.

# Balance opportunities/operations & security risks



# How do we make O365 Secure for us?



O365 Governance

Monthly Security meetings with CISO

Quarterly Meetings with other States

Service Packages

Service Transition Readiness Assessment Checklist (STRAC)

Yearly Service Maturity Assessment

Agency Kickoff meetings for each service

O365 Community of Practice (COPs) / Workgroups

Tenant Owner Guidance

Purchase O365 Government Skus

Must be on a supported OS and Office Version



# O365 Governance – Why?

- Need for a central body to make decisions for the State tenant(s)
- Set Baseline Security
- Provide a 2 way feedback mechanism for policy deployment and impact.
- Multiple services that impact each other
- Change Management and new service coordination and communication
- 40 + Agency domains running in 1 tenant
- Policy and Sharing opportunities between Tenants
  - See [Tenant Owner Guidance](#)
- SLA understanding, negotiation and agreement
- Storage and licensing is pooled and not easily separated by Agency



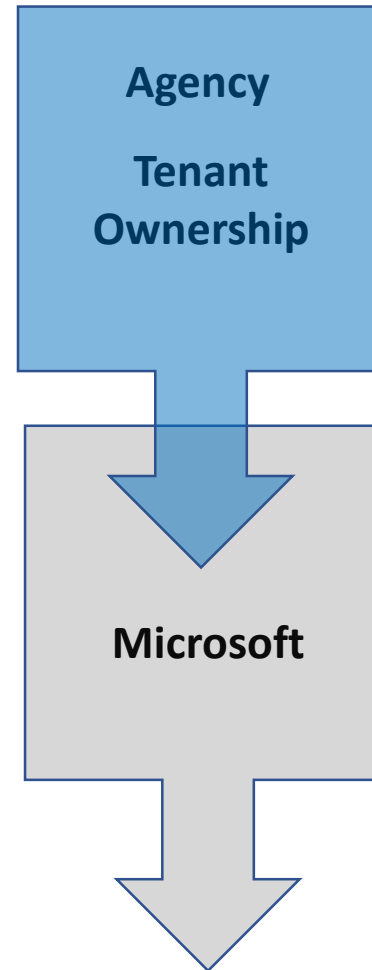
# Community of Practices (COP) Work Groups

- [\*\*O365 Governance\*\*](#)
  - Started 2<sup>nd</sup> year
- [\*\*Email Administrators\*\*](#)
  - Kickoff 11/1 bi-monthly
  - [\*\*COP SP Site\*\*](#)
- [\*\*SharePoint\*\*](#)
  - Started Dec 2016
  - [\*\*COP SP Site\*\*](#)
- [\*\*Power BI Users Group\*\*](#)
  - Started August 2017
  - [\*\*COP SP Site\*\*](#)
- [\*\*Dynamics 365/CRM\*\*](#)
  - Starting November 2018
- [\*\*Desktop/Office Deployment\*\*](#)
  - Started 2<sup>nd</sup> year / As needed
  - [\*\*COP SP Site\*\*](#)
- [\*\*O365 Tenant Owners\*\*](#)
  - Started in 2018
  - [\*\*COP SP Site\*\*](#)



Responsibility	On-Prem	IaaS	PaaS	SaaS
Data classification & accountability	Cloud Customer	Cloud Customer	Cloud Customer	Cloud Customer
Client & end-point protection	Cloud Customer	Cloud Customer	Cloud Customer	Cloud Customer / Cloud Provider
Identity & access management	Cloud Customer	Cloud Customer	Cloud Customer / Cloud Provider	Cloud Customer / Cloud Provider
Application level controls	Cloud Customer	Cloud Customer	Cloud Customer / Cloud Provider	Cloud Provider
Network controls	Cloud Customer	Cloud Customer / Cloud Provider	Cloud Provider	Cloud Provider
Host infrastructure	Cloud Customer	Cloud Customer / Cloud Provider	Cloud Provider	Cloud Provider
Physical security	Cloud Customer	Cloud Provider	Cloud Provider	Cloud Provider

■ Cloud Customer
 ■ Cloud Provider



# Microsoft Responsibility Government Environments

- Store content in the continental United States
- Employ screened US citizens as Microsoft Admins

## Microsoft 365 Government GCC

Best for **FedRAMP Moderate**  
impact data  
Supports **CJIS** and **IRS 1075**  
Complies with **DISA Level 2**  
Security Requirements  
Guidelines

## Microsoft 365 Government GCC High

Best for **FedRAMP High** impact  
data  
Supports **ITAR** and **DFARS**  
Complies with **DISA Level 4**  
Security Requirements  
Guidelines

## Microsoft 365 Government DoD

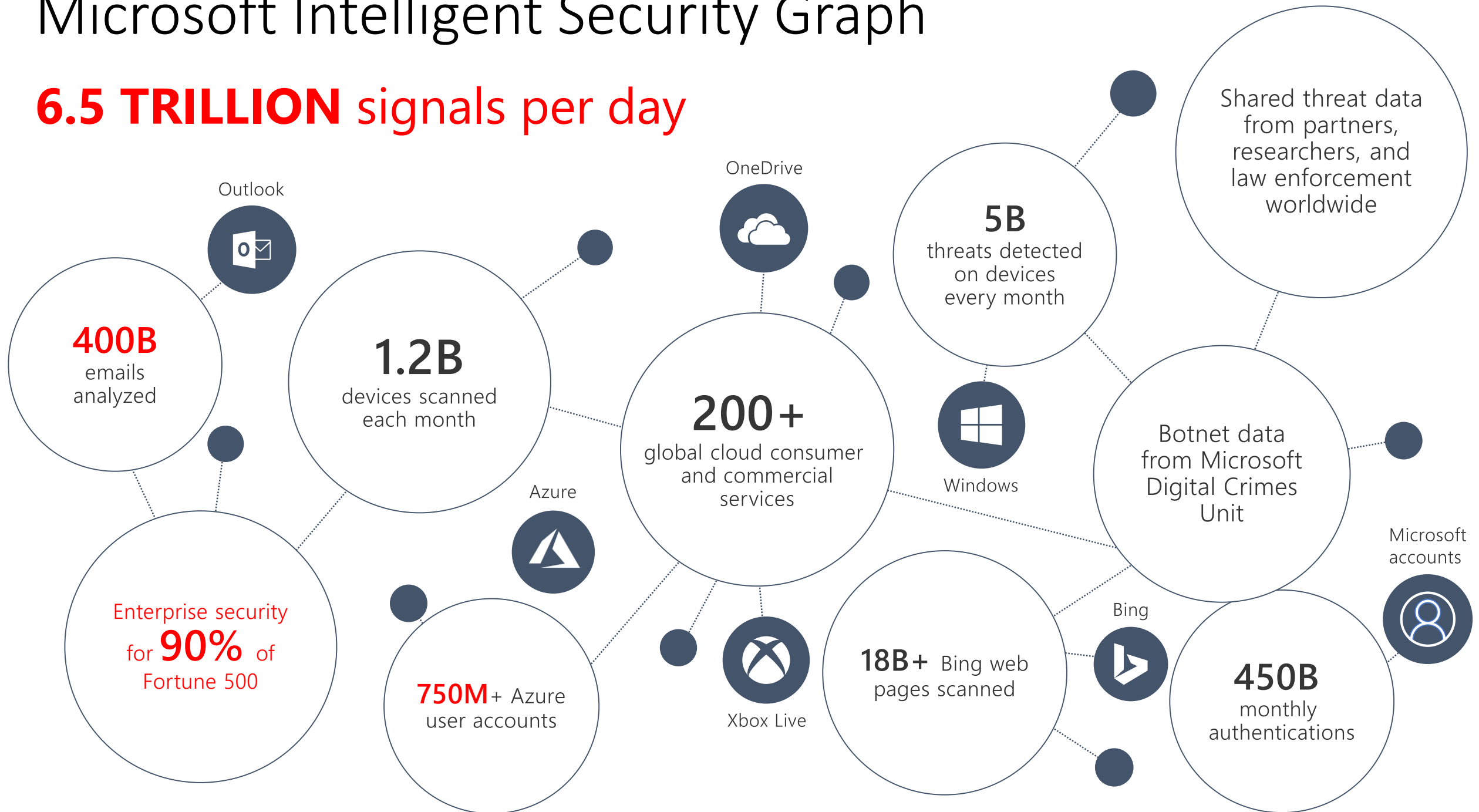
Complies with **DISA Level 5**  
Security Requirements  
Guidelines  
*For exclusive use by US  
**Department of Defense***

**For more information:** <https://technet.microsoft.com/en-us/library/mt774581.aspx>  
**Trust Center:** <https://www.microsoft.com/en-us/trustcenter/default.aspx>



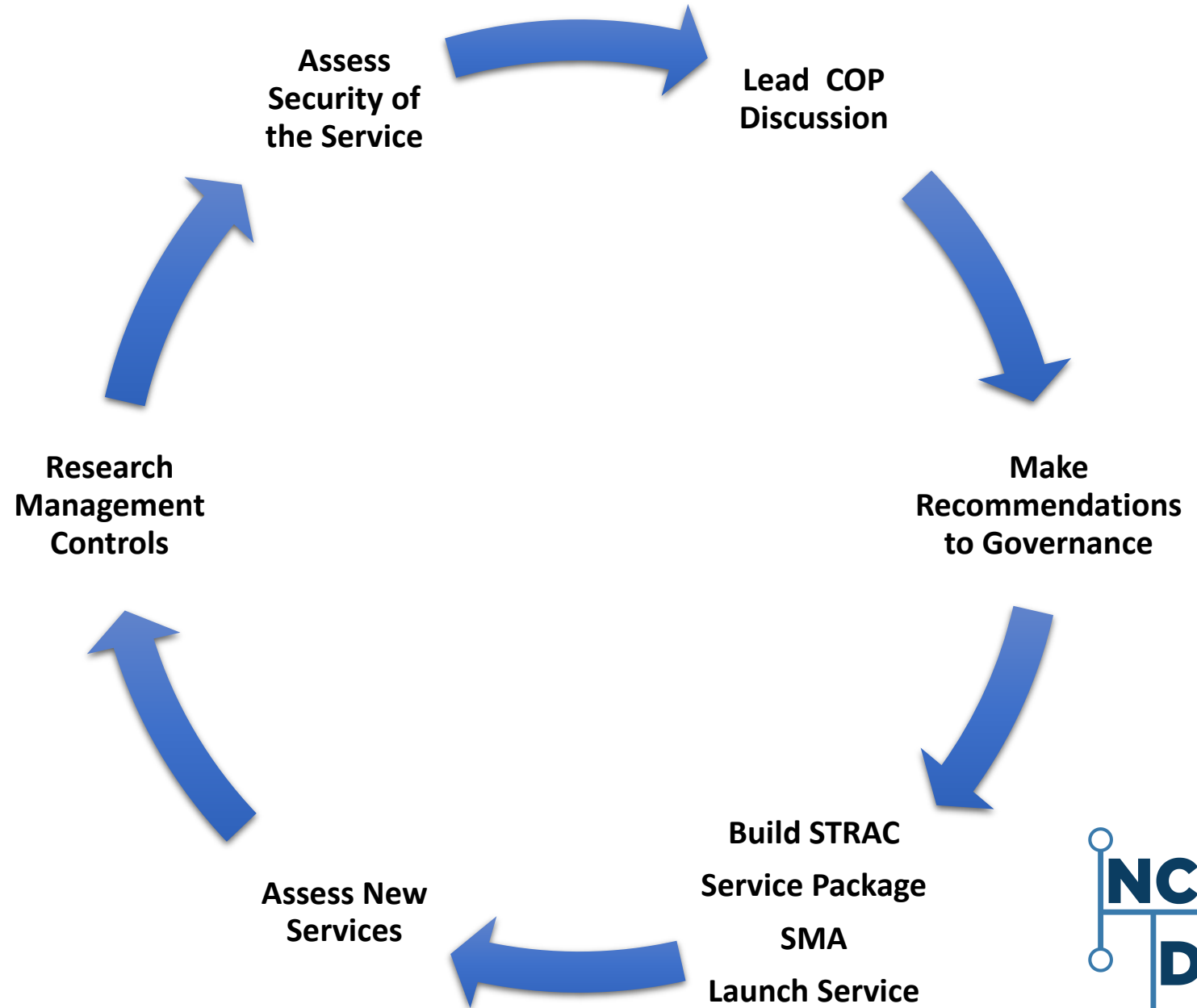
# Microsoft Intelligent Security Graph

**6.5 TRILLION** signals per day



# Tenant Owner Responsibility =

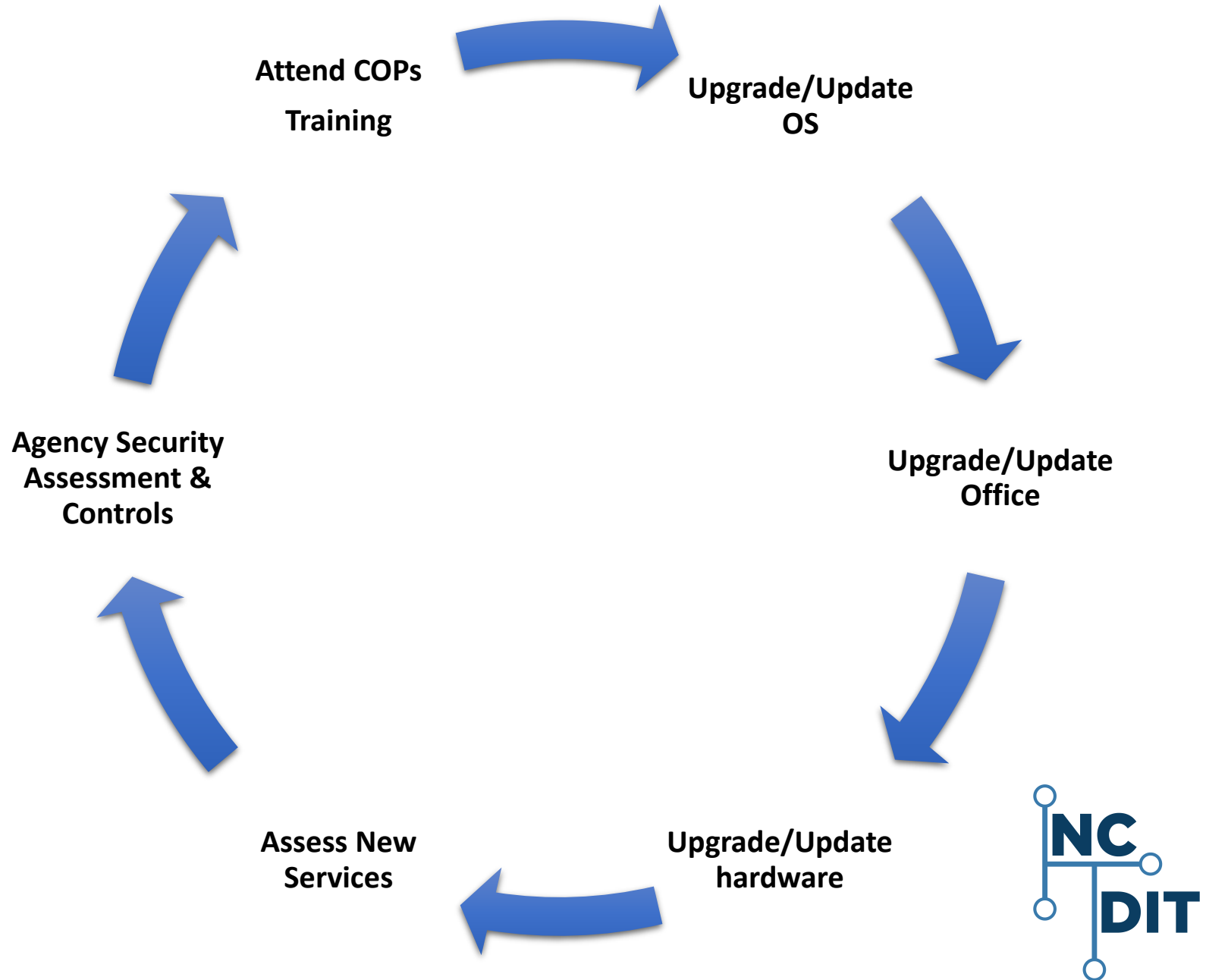
# Manage Constant Change





Agency  
Responsibility =

Manage Constant  
Change



# Agency Responsibility

- Stay up to date (OS, Hardware, Office updates)
- Endpoint Protection
- Data Classification
- Specific Service Decisions & Settings
- Send your Service admins/users to COP to learn what's coming and security best practices
- Practice and Promote Governance and COP Recommendations



1 Year

2 Months

27 Days

# When will support end?



Windows  
XP



Windows  
Vista



Windows  
7



Windows  
8 / 8.1

*Mainstream  
support ends*

14  
April  
2009

10  
April  
2012

13  
January  
2015

9  
January  
2018

*Extended  
support ends*

8  
April  
2014

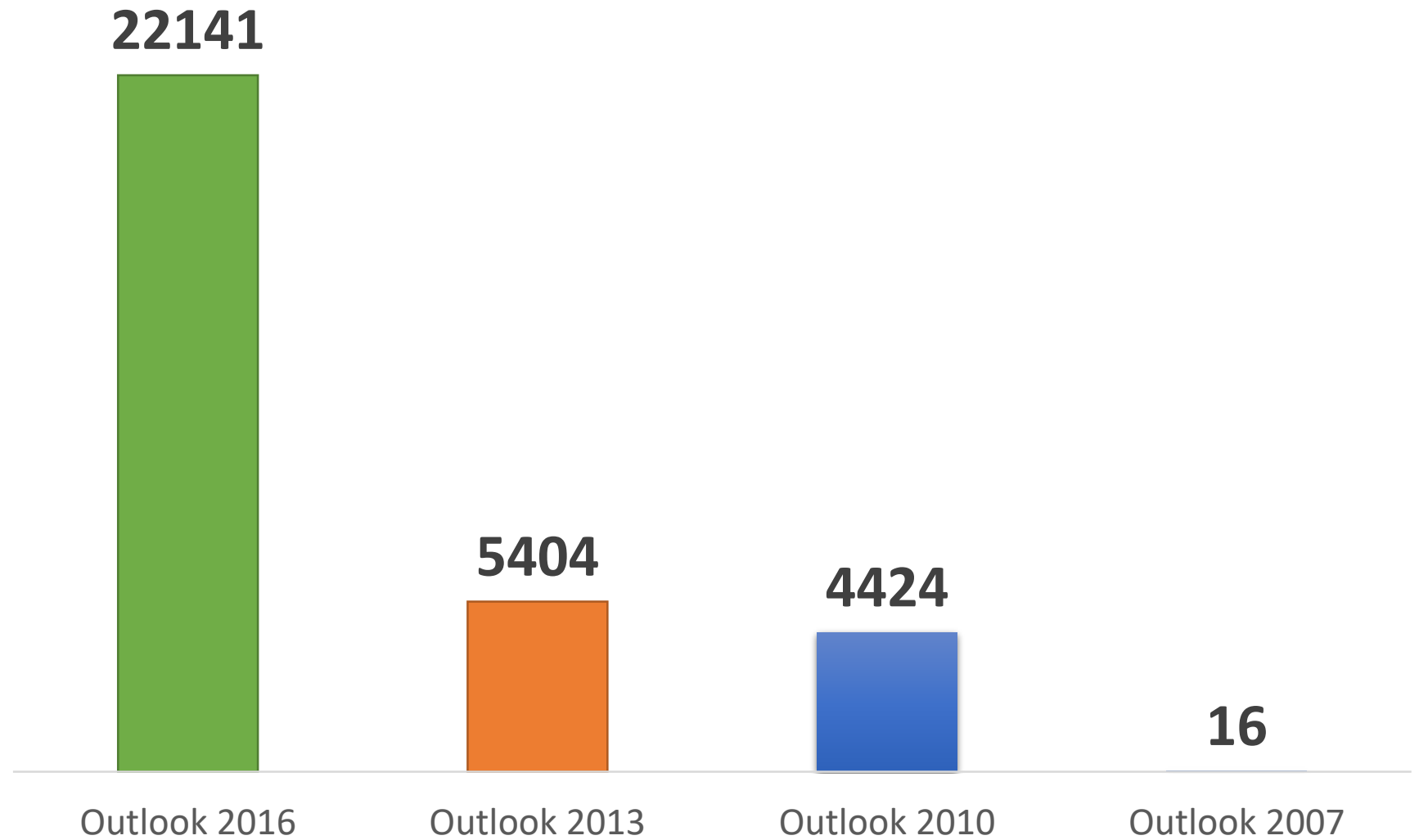
11  
April  
2017

14  
January  
2020

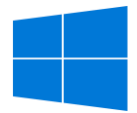
10  
January  
2023



Current OS  
Versions  
DIT Tenant



# What is the Ideal State to consume O365 Services?



Windows 10



OneDrive



Office 365

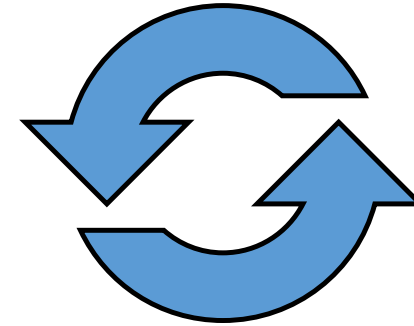




# How many services do we offer in O365?



13 Active



7 Evaluating

# Service Offerings

## Available Offerings



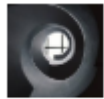
Dynamics 365



Groups



OneDrive for Business



Email



Intune MAM



Planner



Email Filtering/Relay



Mailman



Power BI



Forms



Office Graph/Delve



SharePoint Online

---

## Evaluating Offerings



Cisco Collaboration Suite



StaffHub



Intune MDM



Sway



Microsoft Teams



To Do



PowerApps & Flow

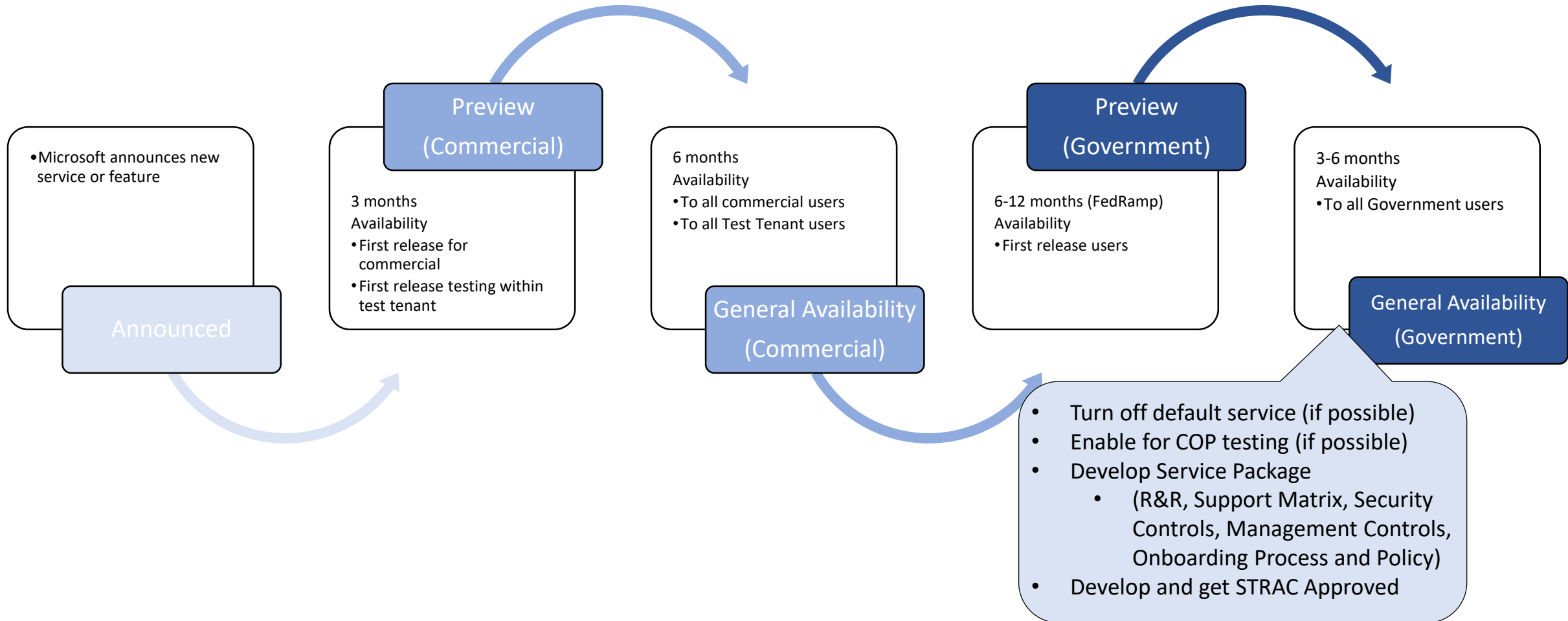


# What's New?

- O365 Groups
- Intune MAM (Mobile Application Management)
- Power BI

# *O365 New Features*

## *From MS Announcement to DIT Tenant Go Live*





# Best Practices

# Email Best Practices



**Use Encryption if  
Needed**



**Use Rights Management**



**DLP is set up for  
PII and PCI**



**Implemented SPF,  
working on DKIM,  
DMARQ**



**Removed Protocols not  
needed on every  
account. IMAP, SMTP,  
POP By default all were  
enabled.**



**Piloting new email  
Security Gateway.**



**Audit all MBX accounts.**



**Train users  
Phishing Simulators**



# Email Encryption and DLP

**Two ways you can trigger an encrypted email:**

## **1. Manually invoking encryption**

Office Message Encryption – Manually send an encrypted email by typing [encrypt] in the subject line when you are working with external users. There must be space on either side of the bracket.

**2. Automatically triggering encryption DLP (Data Loss Prevention) enforced Encryption** - Automatic encryption based on set rules for sensitive data types (SSN/PII and PCI/Credit Card).

Internal emails are automatically encrypted. TLS (Transport Layer Security) v 1.2 protocol for secure communication.



# Email Recommendations -Phishing

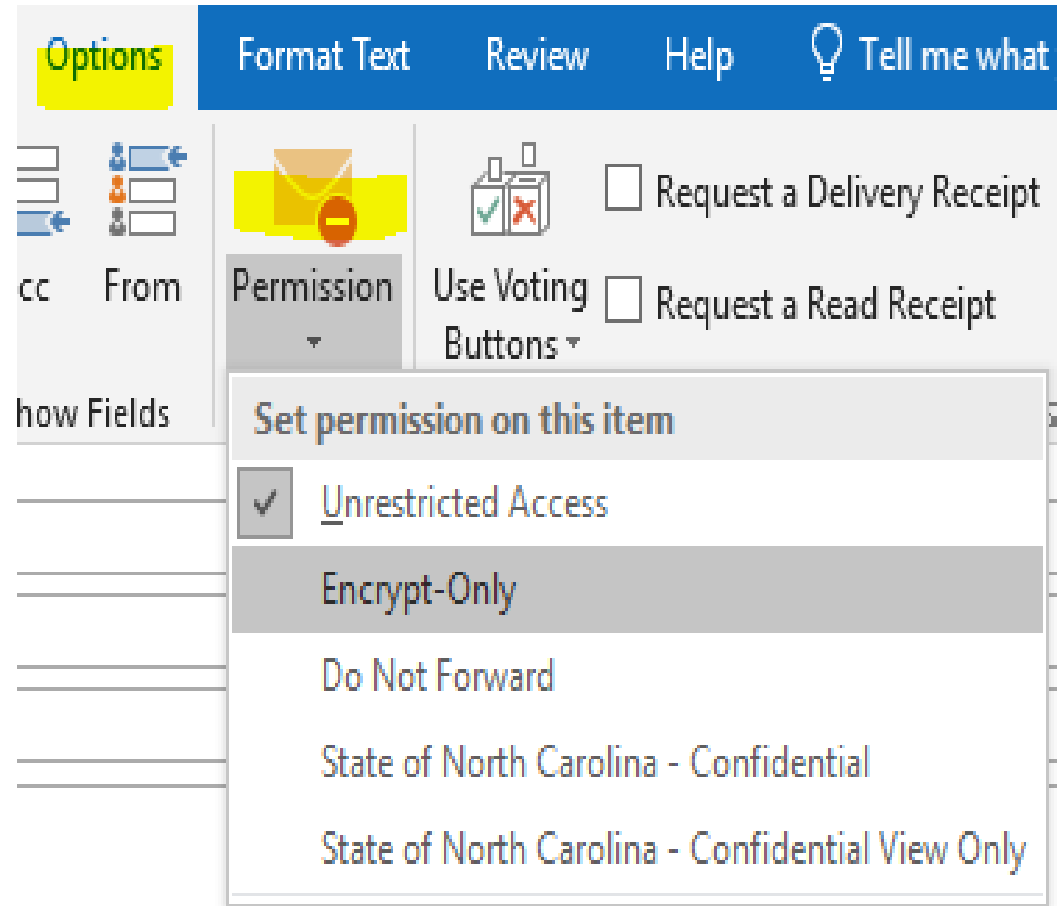
Most secure email gateway vendors are not responding fast enough to increasing levels of phishing attacks.

Security and risk managers (SRMs) should take a three-pronged approach to improving their defenses against phishing attacks:

1. Upgrade secure email gateway and other controls to improve protection for phishing.
2. Integrate employees into the solution and build capabilities to detect and respond to suspected attacks
3. Work with business managers to develop standard operating procedures for handling sensitive data and financial transactions.

# Rights Management Emails

- Rights Management features:  
Do not forward, copy, print
- Some Rights Management Permissions only work for internal users. Ex. Confidential
- Encrypt & Do Not Forward work for External users.



# Mobile Application Management (MAM) Best Practices



**Lock Down MS Applications on the phone.**



**Set min OS level  
Android 6.0/iOS 8.1**



**Block managed apps  
from running on  
jailbroken or rooted  
devices**



**Set App PIN**



**Select which storage  
services State data can  
be saved to  
OneDrive for Business &  
SharePoint**



**Restrict cut, copy and  
paste with other apps.**



**Encrypt data within  
scoped Apps**

# OneDrive/SharePoint Best Practices



**Move to Modern Sites  
vs Classic SharePoint**



**Use IRM for Sensitive  
Document Libraries**

**Set up DLP**



**Lock down creation of  
sites and O365  
Groups/Teams**



**Block downloads for  
sensitive documents.**  
Prevent users from  
downloading & copy and  
pasting documents.



**Only allow external  
sharing from specific  
sites and by Admins**

**Set up a Private Folder  
in OneDrive**



**Sensitive data in Lists  
and Libraries should be  
excluded from  
Search/Delve**

**Default is include in  
Search**



**Set document / Link  
expiration**  
**Default is 14 days**



**Move to Office 2016 and  
Win 10 or use Browser.**

# Security Controls to Protect Sensitive Data in SharePoint and OneDrive

- How to exclude items from SharePoint Search
- How to disable downloading of documents from SharePoint
- Working with Information Rights Management – Techniques/Tools
- MS Office Protections
- Working with Data Loss Prevention/Policies



## Information Rights Management (IRM)

IRM helps protect sensitive files from being misused or distributed without permission once they have been downloaded from this library.

- ☒ Restrict permissions on this library on download


Create a permission policy title

Add a permission policy description:

HIDE OPTIONS

### Set additional IRM library settings

This section provides additional settings that control the library behavior.

- ☐ Do not allow users to upload documents that do not support IRM
- ☐ Stop restricting access to the library at  
 
- ☐ Prevent opening documents in the browser for this Document Library

### Configure document access rights

This section control the document access rights (for viewers) after the document is downloaded from the library; read only viewing right is the default. Granting the rights below is reducing the bar for accessing the content by unauthorized users.

- ☐ Allow viewers to print
- ☐ Allow viewers to run script and screen reader to function on downloaded documents
- ☐ Allow viewers to write on a copy of the downloaded document
- ☐ After download, document access rights will expire after these number of days (1-365)

### Set group protection and credentials interval

Use the settings in this section to control the caching policy of the license the application that opens the document will use and to allow sharing the downloaded document with users that belong to a specified group

- ☐ Users must verify their credentials using this interval (days)
- ☐ Allow group protection. Default group:

## Link settings

Document 1.docx



Who would you like this link to work for? [Learn more](#)



Anyone



People in State of NC



People with existing access



Specific people

Other settings

- ☒ Allow editing

 Expires Tuesday Nov 6 2018



November 2018



S	M	T	W	T	F	S
28	29	30	31	1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	1

# DLP in SP and OD & How this works

- PII and PCI Customized Sensitive Data Templates enabled
- Monitoring and notifying. Not enforcing DLP policies yet.
- Send an incident report to the security liaison and notify the content owners with a Policy Tip if sensitive data is detected.
- Support for DLP and hits on Sensitive Data in Exchange, SharePoint and OneDrive need to be directed to the Agency Security Liaison.
- *In order to see Policy Tips, Users need to use OWA or have 2013 or later Office ProPlus*



# Restore OneDrive file

## Restore your OneDrive

If something went wrong, you can restore your OneDrive to a previous time. Select a date preset or use the slider to find a date with unusual activity in the chart. Then select the changes that you want to undo.

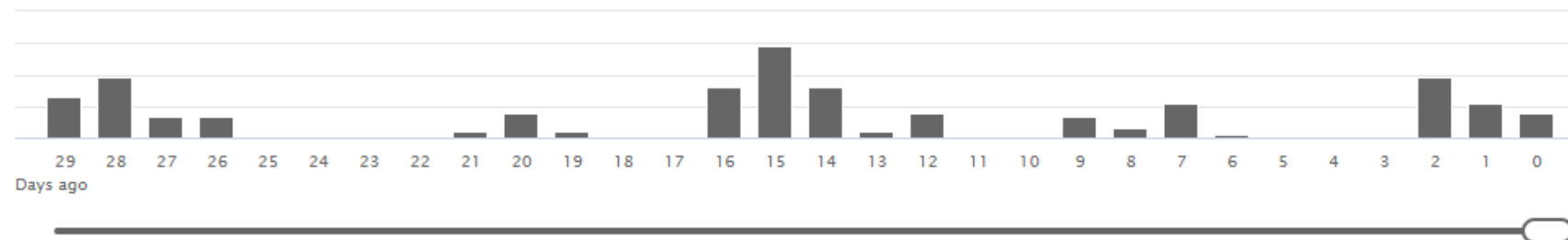
Select a date

Custom date and time

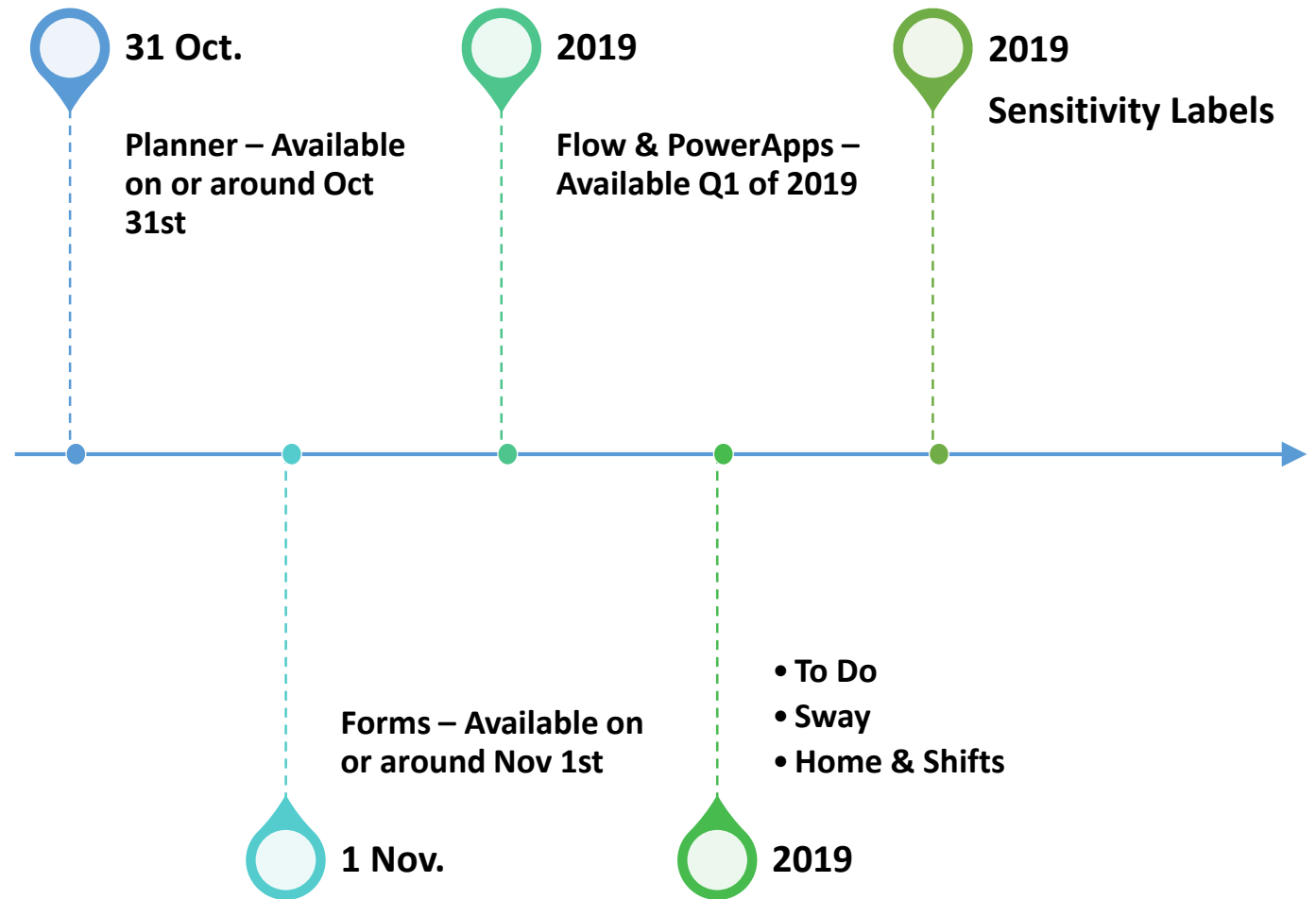
Restore

Cancel

Move the slider to quickly scroll the list to a day.



# Coming Soon – Major Features



More info?

<https://ncconnect.sharepoint.com/sites/O365/SitePages/Home.aspx>

# FUTURE APPROACH TO **INFORMATION PROTECTION**

Comprehensive protection of sensitive data throughout the lifecycle – inside and outside the organization



## Detect

Scan & detect sensitive data based on policy



## Classify

Classify data and apply labels based on sensitivity



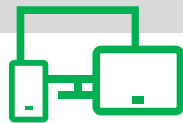
## Protect

Apply protection actions, including encryption, access restrictions



## Monitor

Reporting, alerts, remediation



DEVICES



CLOUD



# SENSITIVITY LABELS PERSIST WITH THE DOCUMENT

## Document labeling – what is it?

Metadata written into document files

Travels with the document as it moves

In clear text so that other systems such as a DLP engine can read it

Used for the purpose of apply a protection action or data governance action – determined by policy

Can be customized per the organization's needs



## More info?

<https://docs.microsoft.com/en-us/Office365/SecurityCompliance/sensitivity-labels>

## Admin

- Creates a sensitivity label
- Publishes the sensitivity label to users and groups selected in a label policy

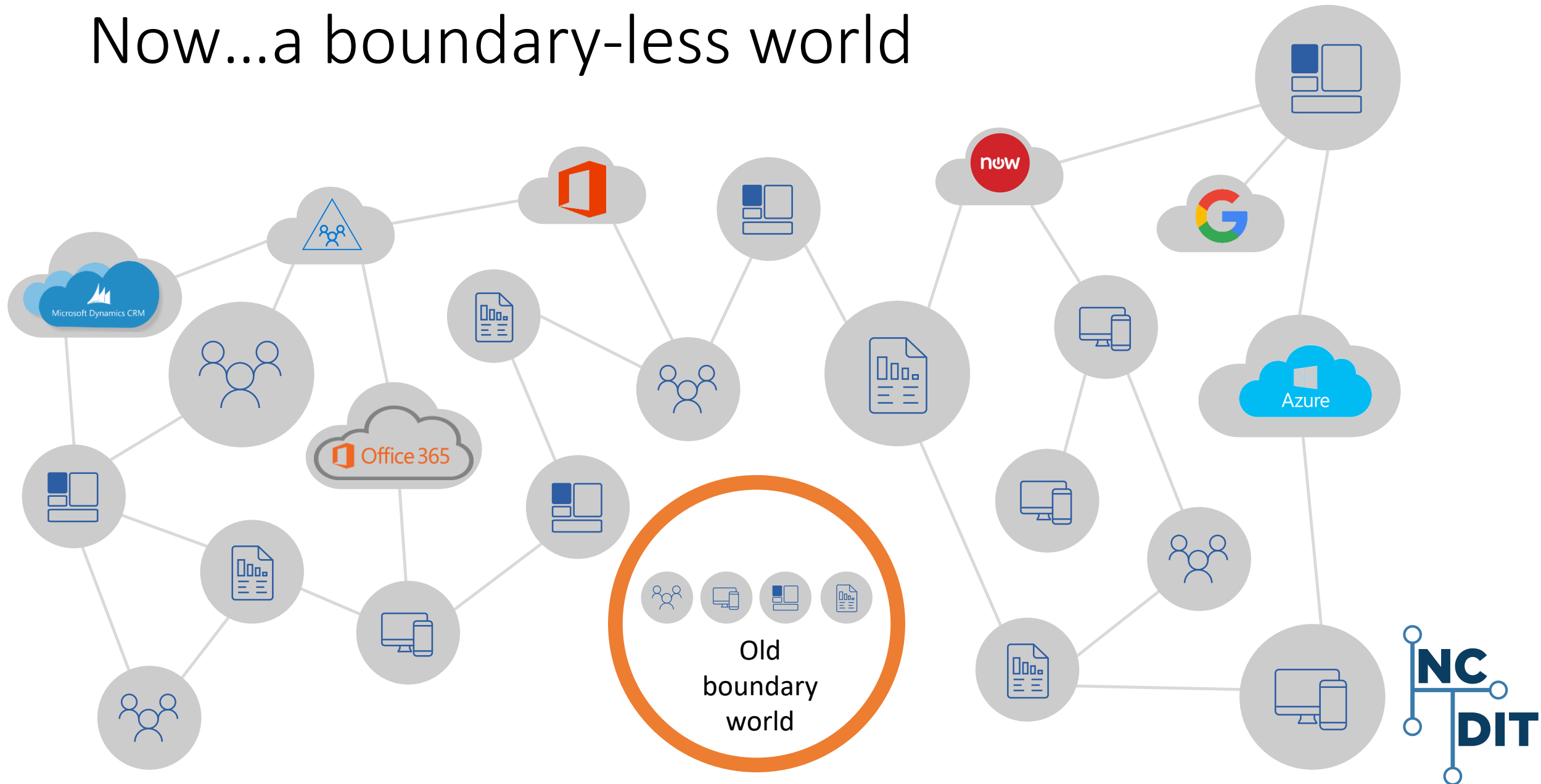
## End user

- Works on an email or document and sees the available labels
- Classifies the document by applying a label

## Office or third-party app/service

- Enforces protection settings on the email or document based on the applied label

# Now...a boundary-less world







# PROTECT SENSITIVE DATA ACROSS THE ENVIRONMENT

## Devices

Drive encryption ✓

MAM/ Remote wipe ✓

MAM/ Business data separation ✓



## Cloud

✓ File encryption

✓ Secure External Sharing

✓ Permissions and rights-based restrictions

✓ DLP actions to prevent sharing

✓ Policy tips & notifications for end-users

✓ Visual markings in documents

✓ Control and protect data in cloud apps with granular policies and anomaly detection

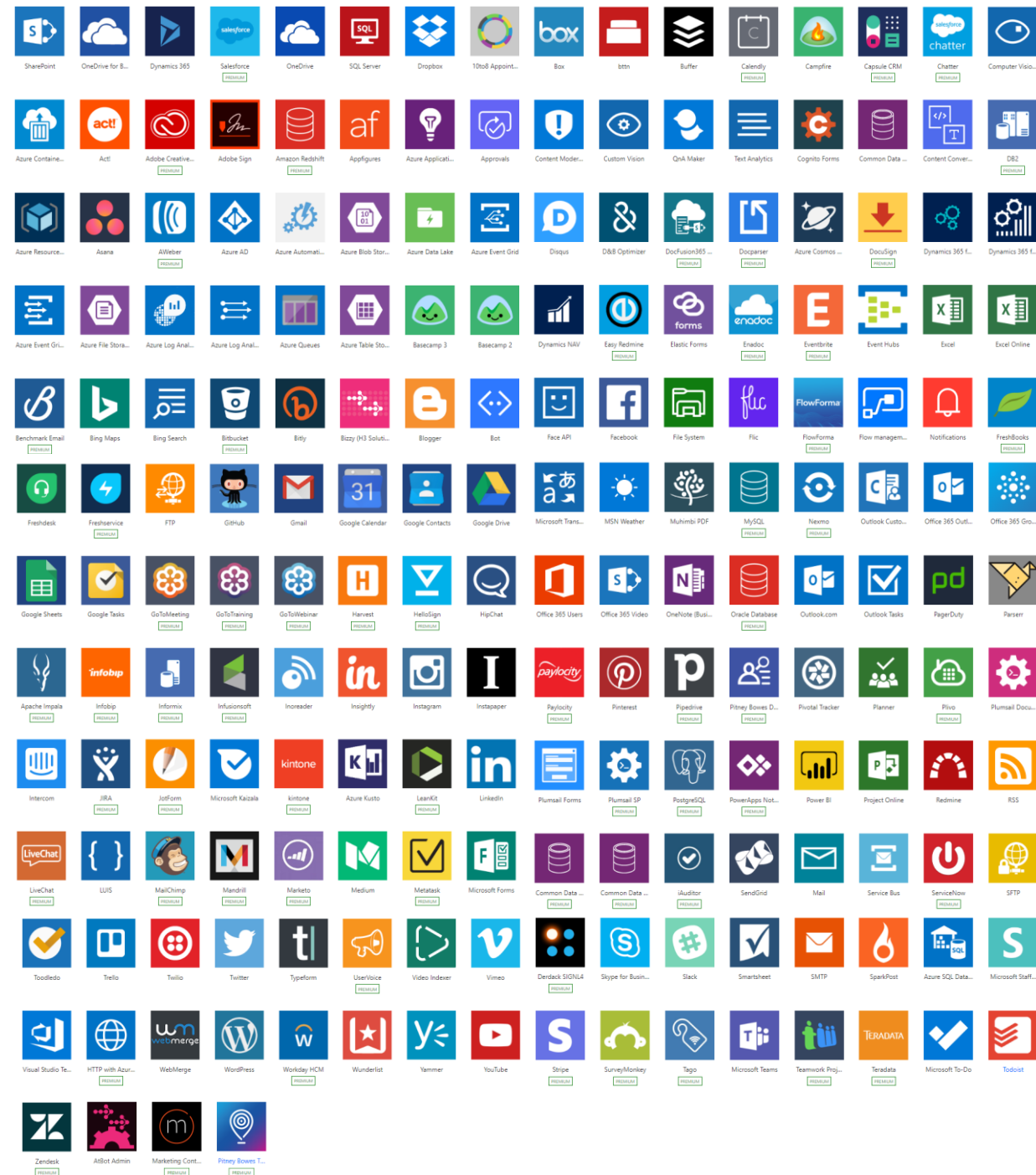
✓ Data retention, expiration, deletion

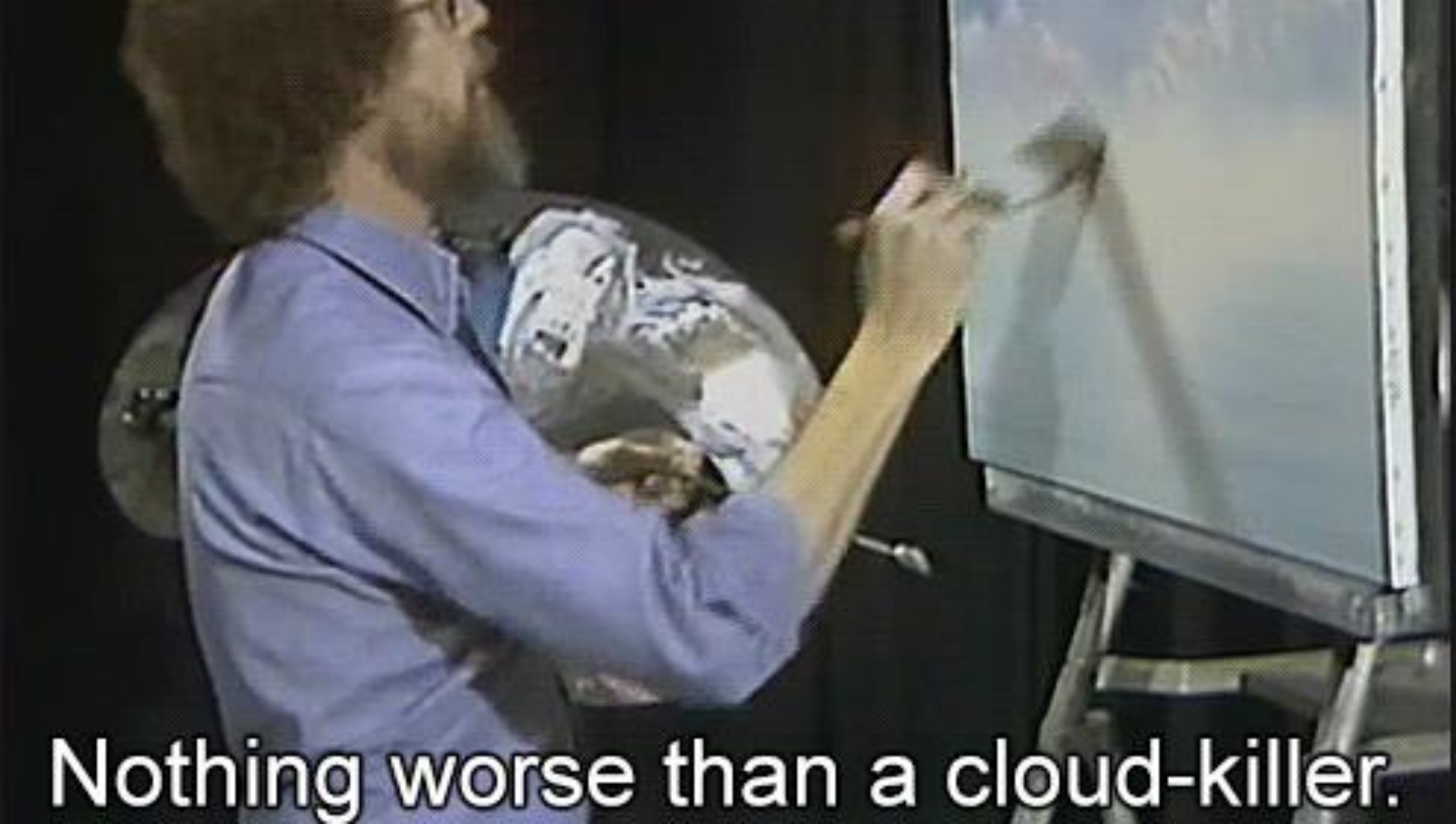


# What's Our Next Challenge?

## Power Apps and Flow

- Built-in connectivity to 230+ SaaS cloud services, file providers, databases, web APIs, productivity apps, and more
- Connect to on-premises systems via Data Gateway
- Pluggable extensibility via Custom Connectors to integrate existing LOB systems into Flow





Nothing worse than a cloud-killer.



Cybersecurity is a **Shared** Responsibility!



Q & A



Contact us



**Contact your BRM  
or**

**send an email to**

[O365SME@nc.gov](mailto:O365SME@nc.gov)

[Office 365 Service Packages,  
Training & Support](#)

[O365 Governance Site](#)

[Tenant Owners Site](#)